Object moved to here.

Object moved to here.

NSA Documents: Attacks on VPN, SSL, TLS, SSH, Tor

December 28, 2014 – 08:04 PM

Print | E-Mail

Feedback

NSA Spying Scandal

Attacks against Crypto

- Guide for Analysts on how to use the PRISM Skype Collection
- GCHQ Briefing on the BULLRUN Program
- GCHQ Presentation on the BULLRUN Programs Decryption Capabilities
- NSA LONGHAUL program for end-to-end attack orchestration and key recovery service
- BLUESNORT program on "Net Defense" from Encrypted Communications
- Presentation from the SIGDEV Conference 2012 explaining which encryption protocols and techniques can be attacked and which not
- NSA program SCARLETFEVER explaining how attacks on encrypted connections are orchestrated
- Description of VOIP Telephony Encryption methods and cryptanalytic and other ways to attack

Attacks on SSL/TLS

- NSA Experiment for massive SSL/TLS Decryption
- Canadian Document from CES on TLS Trends
- Details on how NSA uses the SCARLETFEVER program to attack Scure Sockets Layer (SSL)/Transport Layer Scurity (TLS)
- Analysis from SSL/TLS Connections through GCHQ in the flying pig database

Attacks on VPN

- NSA High Level Description on TURMOIL / APEX Programs on Attacking VPN
- Explanation of the GALLANTWAVE that decrypts VPN Traffic within LONGHAUL
- Intro to the VPN Exploitation Process mentioning the protocols attacked - PPTP, IPSEC, SSL, SSH)
- Analytic Challenges from Active-Passive Integration when NSA attacks IPSEC VPNs
- Overview of the capabilities of the VALIANTSURF program
- MALIBU Architecture Overview to exploit VPN Communication
- POISENNUT Virtual Private Network Attack Orchestrator (VAO)
- NSA Presentation on the development of Attacks on VPN
- NSA Presentation on the Analysis and Contextualisation of data from VPN
- Description of existing projects on VPN decryption
- Explanation of the Transform Engine Emulator when attacking VPN
- Explanation of the POISENNUT Product and its role when attacking VPN
- Explanation of the TURMOIL GALLANTWAVE Program and its role when attacking VPN
- Processing of data from exploited VPN in the TURMOIL program
- Decryption of VPN Connections within the VALIANTSURF program
- Description on the processing of VPN data packets within the TURMOIL program
- Explanation on the SPIN9 program on end-to-end attacks on VPN

Deanonymizing

- Explanation of a potential technique to deanonymise users of the TOR network

Twitter

Analytics on security of TOR hidden services

Overview on Internet Anonymization Services on how they work

TOR deanonymisation research

TOR Overview of Existing Techniques

A potential technique to deanonymise users of the TOR network

Cryptanalytics

General Description how NSA handles encrypted traffic

Intercept with PGP encrypted message

Classification Guide for Cryptanalysis

Procedural GCHQ Document on how analysts are to handle encrypted traffic

NSA / GCHQ Crypt Discovery Joint Collaboration Activity

NSA Cryptographic Modernization (CryptoMod) Classification Guide

"National Information Assurance Research Laboratory (NIARL)": Newsletter, Keyword TUNDRA

What Your Mother Never Told You About the development of Signal Intelligence

Intercept with OTR encrypted chat

Article...

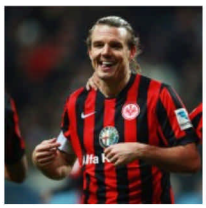
Print | **E-Mail** Feedback

Das könnte Sie auch interessieren

BVB auf Abstiegsplatz

Borussia Dortmund verpflichtet Kampl

Der BVB steckt in der Krise. Nun hat der Klub reagiert - und auf dem Transfermarkt zugeschlagen: Der slowenische Nationalspieler Kevin Kampl wechselt von RB Salzburg nach Dortmund. Ein anderer Profi hat die Borussia verlassen. mehr...



Bundesliga-Goalgetter Alex Meier

Stehen, warten - Tor

Der beste Bundesliga-Torjäger spielt nicht bei Bayern München oder beim VfL Wolfsburg, sondern bei Eintracht Frankfurt: Alexander Meier trifft, wie er will. Viel laufen muss er dafür nicht mehr. mehr...

Borussia Dortmund

Langerak bis zur Winterpause im BVB-Tor

Weltmeister Roman Weidenfeller auf der Bank, Ersatzkeeper Mitchell Langerak im Tor: Das wird bei Borussia Dortmund erst einmal so bleiben. Trainer Jürgen Klopp legte sich auf den Australier als Nummer eins für den Rest der Hinrunde fest. mehr...

Spionage

Falsche Mobilfunkstationen im norwegischen Regierungsviertel entdeckt

Norwegens Politiker werden offenbar von Unbekannten ausspioniert. Rund um zentrale Regierungsgebäude in Oslo hat eine Zeitung Überwachungsgeräte entdeckt. Der Geheimdienst ist beunruhigt. mehr...

Keep track of the news

Stay informed with our free news services:

MORE FROM SPIEGEL INTERNATIONAL

GERMAN POLITICS

Merkel's Moves: Power Struggles in Berlin

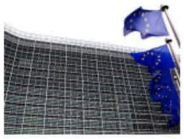
WORLD WAR II

Truth and Reconciliation: Why the War Still Haunts Europe

ENERGY

Green Power: The Future of Energy

EUROPEAN UNION



United Europe: A Continental Project

CLIMATE CHANGE

Global Warming: Curbing Carbon Before It's Too Late

OVERVIEW INTERNATIONAL ▶

▲ TOP

Home Politik Wirtschaft Panorama Sport Kultur Netzwelt Wissenschaft Gesundheit einestages Uni Reise Auto Stil Wetter

DIENSTE
Schlagzeilen
Nachrichtenarchiv
RSS
Newsletter
Mobil

VIDEO
Nachrichten Videos
SPIEGEL TV Magazin
SPIEGEL TV Programm
SPIEGEL Geschichte
SPIEGEL TV Wissen

MEDIA
SPIEGEL QC
Mediadaten
Selbstbuchungstool
weitere Zeitschriften

MAGAZINE
DER SPIEGEL
Dein SPIEGEL
SPIEGEL GESCHICHTE
SPIEGEL WISSEN
KulturSPIEGEL
UniSPIEGEL

SPIEGEL GRUPPE
Abo
Shop
SPIEGEL TV
manager magazin
Harvard Business Man.
buchreport
buch aktuell
Der Audio Verlag
SPIEGEL-Gruppe

WEITERE
Hilfe
Kontakt
Nutzungsrechte
Datenschutz
Impressum

▲ TOP